

INFORMATION SECURITY POLICY

Confidential

1. Purpose

The document aims to better establish management direction by laying the necessary procedures to help safeguard confidentiality, integrity and availability of all of its business assets.

2. Objectives

This document was written with the following considerations in mind:

- To establish safeguards to protect information resources from theft, abuse, misuse and any form of damage and establish responsibility and accountability for Information Security in the organisation.
- To create an appropriate level of awareness, knowledge and skill to allow both staff and management to minimise the occurrence and severity of Information Security incidents.
- To set out a culture of data protection and privacy across the organisation.

This policy should be read in conjunction with all other company Policies and Procedures.

All Policies and Procedures are subject to an annual revision where documents are updated if necessary in order to ensure that all documents are true to the organisation's current operation.

3. Responsibilities

3.1 Information Security Manager

For the purpose of this document, the role of Information Security Manager has been entrusted to the CEO at the outset, and following this, a dedicated Information Security Manager will be employed. Such person is responsible for protecting and safeguarding data, maintaining the Information Security Policy and in charge of Risk Management related to data.

The Information Security Manager will also be in charge of enforcing this policy and ensure that adequate training/advice is given to new staff who should be aware of the information security best practices and procedures as outlined in this and any other relevant documents.

3.2 Team Effort

To be effective, there should be a team effort involving the participation and support of every employee who deals with information and information systems. In recognition of the need for teamwork, this policy statement clarifies the responsibilities of users and the steps they must take to help protect information and information systems.

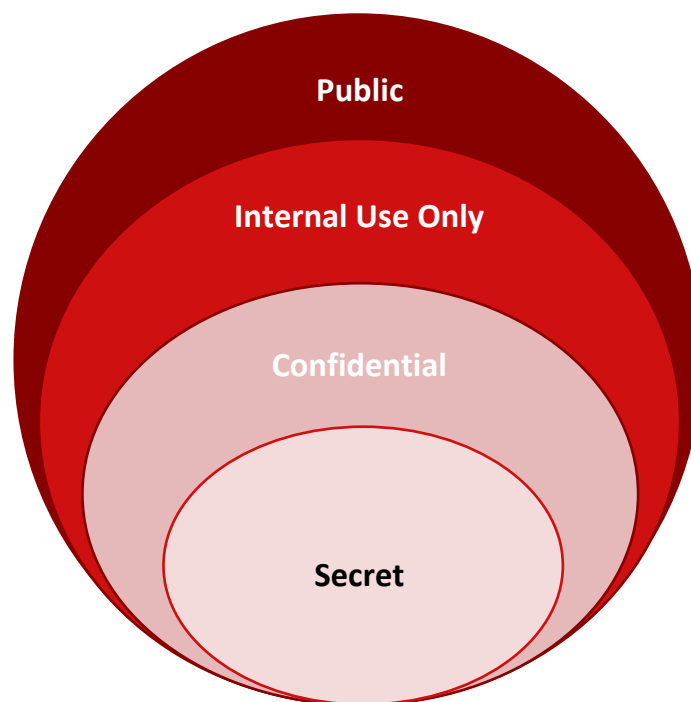
4. Policy

4.1 Safeguarding of data

Information is a vital asset and all accesses to, uses of, and processing of information must be consistent with policies and standards.

Information that has been entrusted to the company must be protected in a manner commensurate with its sensitivity and criticality. Security measures must be employed regardless of the media on which information is stored, the systems that process it, or the methods by which it is moved. Information must be protected in a manner that is consistent with its classification, no matter what its stage in the life cycle from origination to destruction.

4.2 Classification of Data



The Company has adopted an information classification system that categorises information into four groupings. All information under the Company's control, whether generated internally or externally, falls into one of these categories; all workers must familiarise themselves with the definitions and the steps that must be taken to protect the information falling into each of these categories.

Public - This information has been specifically approved for public release and unauthorised disclosure of this information will not cause problems for the Company, its customers, or its business partners. Examples are marketing brochures and material posted to the web page. Disclosure of information to the public requires the existence of this label, the specific permission of senior management, or long-standing practice of publicly distributing this information.

Internal Use Only - This information is intended for use within the organisation, and in some cases within affiliated organizations, such as with our business partners. Unauthorized disclosure of this information to outsiders may be against laws and regulations, or may cause problems for the company, its customers, or its business partners. This type of information could already be widely distributed within the company, or it could be so distributed within the organisation without advance permission from Management. Examples are the Company's book of contact information and most internal electronic mail messages.

Confidential - This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Unauthorized disclosure of this information to people without a business need for access may be against laws and regulations, or may cause significant problems for the Company, its customers, or its business partners. Decisions about the provision of access to this information must be cleared through the information Owner. Examples are customer transaction account information and worker performance evaluation records. Correspondence with the regulator will be treated as confidential information.

Secret - This information is the most private or otherwise sensitive, and must be monitored and controlled at all times. Unauthorized disclosure of this information to people without a business need for access may be against laws and regulations, or may cause severe problems for the Company, its customers, or its business partners. Decisions about the provision of access to this information must be cleared through the Senior Management. Examples are player personal information, source of funds documentation, gambling patterns when these can be linked to specific players (this should always remain anonymous) .

Default Category - If information is not marked with one of these categories, it will default into the **Internal Use Only** category. If information falls into the Internal Use Only category, it is not necessary to apply a sensitivity label. Information that falls into the Confidential or Secret categories is designated Sensitive.

4.3 Safeguarding Applications

Computers and networks should not run software that comes from sources other than business partners, knowledgeable and trusted user groups, well-known systems security authorities, computer or network vendors, or commercial software vendors approved by us. Software downloaded from electronic bulletin boards, shareware, public domain software, and other software from un-trusted sources should not be used unless it has been subjected to a rigorous testing regimen approved by the Information Security Department.

Virus Screening - All personal computers must have the current versions of approved virus screening software enabled. Users must not abort automatic software processes that update virus signatures and periodically scan the terminals. Virus screening software must be used to scan all software and data files coming from either third parties. This scanning must take place before new data files are opened and before new software is executed. Workers must not bypass or turn off the scanning processes that could prevent the transmission of computer viruses.

Virus detection - If workers suspect infection by a computer virus, they must immediately stop using the involved computer and the Information Security department. Any portable storage media used with the infected computer must not be used with any other computer until the virus has been successfully eradicated. The infected computer must also be immediately isolated from internal networks. Users must not attempt to eradicate viruses themselves, but a qualified member of staff or consultants must complete this task in a manner that minimizes both data destruction and system downtime.

4.4 Portable Computers

Employees in the possession of a portable device; example a laptop, notebook, handheld, and other portable computers containing *Confidential* or *Secret* information must not leave these computers unattended at any time unless the information is stored in encrypted form.

Employees in the possession of portable computers containing unencrypted *Confidential* or *Secret* information must not check these computers in airline luggage systems or with hotel porters; however these computers must remain in the possession of the traveller as hand luggage.

Whenever *Confidential* or *Secret* information is written to a portable storage device, the storage media must be suitably marked with the highest relevant sensitivity classification. When not in use, this media must be stored in a locked safe, locked furniture, or a similarly secured location.

4.5 Remote Printing

Printers must not be left unattended if *Confidential* or *Secret* information is being printed or soon will be printed. The persons attending the printer must be authorised to examine the information being printed.

Unattended printing is permitted if the area surrounding the printer is physically protected such that persons who are not authorised to see the material being printed may not enter.

4.6 Safeguarding of Networks

Network is safeguarded by state-of-the-art network firewall device. The firewall is “transparent”, meaning it protect the servers with the public IP addresses and allows only network traffic which is for the purpose of providing service. All other network traffic is denied by default.

Logs containing computer or communications system security relevant events should be retained for at least three months. During this period, logs should be secured such that they cannot be modified, and such that only authorised persons can read them.

The relevant information should be captured whenever it is suspected that computer or network related crime or abuse has taken place. The relevant information should be securely stored offline until such time as it is determined that the Company will not pursue legal action or otherwise use the information. The information to be immediately collected should include system logs, application audit trails, other indications of the current system states, and copies of all potentially involved files. Records reflecting security relevant events should be periodically reviewed in a timely manner.

Users must be informed of the specific acts that constitute computer and network security violations. Users must also be informed that such violations will be logged.

Although system administrators are not required to promptly load the most recent version of operating systems, they are required to promptly apply all security patches to the operating system that have been released by knowledgeable and trusted user groups, well-known systems security authorities, or the operating system vendor. Only those systems security tools supplied by these sources or by commercial software organizations may be used on computers and networks.

Handling Network Security Information - From time to time, the Information Security Manager will designate individuals to audit compliance with this and other computer and network security policies. At the same time, every worker must promptly report any suspected network security problem, including intrusions and out-of-compliance situations, to the Information Security manager.

4.7 Safeguarding of Equipment

In addition protection from fire, floods, earthquakes, or any forms of natural or man-made disasters, Office and Production environments should contain physical security barriers, such as biometrics and / or card-controlled entry systems.

Access to systems should only be granted by entering unique credentials, which identifies each member of staff. The use of generic credentials is strongly discouraged by the company.

All critical equipment should be protected and maintained by making use of devices such as an Uninterrupted Power Supply (UPS) in case of power failure and Surge protectors to avoid damage to equipment when there is a fluctuation in electricity.

Equipment should also be given situated in an appropriate air-Conditioned environment.

4.8 Disposal of Equipment / Media

When sensitive information is erased from a disk, tape, or other reusable data storage media, it must be followed by a repeated overwrite operation in order to obliterate the sensitive information.

Before any computer storage media is sent to a vendor for trade-in, servicing, or disposal, all sensitive information must be destroyed or concealed according to methods approved by the Information Security Manager.

The disposal of all paper documents that contain payment information such as bank account numbers or credit card numbers, must involve shredding or other approved destruction methods.

Equipment which needs to be securely disposed of has to follow the correct procedure (refer to the Incident Response & Asset Removal Policy).

4.9 Enforcement

Every member of staff must comply with the information security policies found in this and related information security documents. Staff who deliberately violate this and other information security policy statements will be subject to disciplinary action up to and including termination.